INFORMATION MANAGEMENT MANUAL

The Information Management Department welcomes you to CarePlus New Jersey.

Part of the Information Management and Technology Departments' role is to provide you with the information-based tools to help you perform your job responsibilities. These tools may be in the form of computer equipment (hardware), programs (software), training, reports and/or maintenance.

SECURITY/CONFIDENTIALITY

CarePlus New Jersey is a private, non-profit, community-based agency providing mental health and substance abuse treatment.

A "therapeutic relationship" exists between the client and the agency, therefore, all agency staff are considered bound by that relationship. This includes full time and part time staff, volunteers, interns and subcontractors.

Any reference or directive in this document to "staff" or "employees" regarding the security and confidentiality of information also includes volunteers, interns and subcontractors who are providing care and/or services to any CarePlus New Jersey client.

All agency staff is required by law and by practice standards to protect our clients' right to privacy.

All identifiable client information whether it is verbal or written, stored on hardcopy or electronically is to be considered protected. This includes a client's name, address, social security number, condition, date of treatment, etc.

Electronically stored client information is secured physically, electronically and administratively.

In addition, CarePlus assures the confidentiality of all of its Medical Records, Human Resources, Payroll, Fiscal, Research, Information Systems and Management information (collectively known as "Confidential Information").

SANCTION POLICY

Security is the responsibility of everyone.

A security incident (security breach) is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

A breach of security is considered a serious violation of policy and anyone who breaches security will be subject to progressive discipline up to and including dismissal, termination of business contract, and reporting the violation to licensing and law enforcement officials.

IT IS A SERIOUS BREACH OF SECURITY TO SHARE YOUR LOGIN NAME AND PASSWORD WITH ANYONE.

HIPAA SECURITY

Put simply any user of electronically stored Protected Health Information is required to comply with all CarePlus New Jersey policies to make sure that a situation is not created where information is seen by someone who should not have access to it, is corrupted or is rendered unavailable.

If you have any questions about security, contact your supervisor or the CarePlus New Jersey Associate VP of Quality Assurance & Information Management. The Associate VP of Quality Assurance & Information is the Agency's designated security contact designee.

SECURITY CONTACT DESIGNEE INFORMATION

William Maslak
Associate VP Quality Assurance & IM/Privacy Officer
Phone: 201-843-5218
E-mail: williamm@careplusnj.org

The Agency's security contact designee needs to know whether security policies and procedures are being violated or whether you notice something unusual that you think may represent a security problem.

ELECTRONIC POLICY

The CarePlus New Jersey Electronic Policy, specifically addresses the use of Agency equipment and business communication methods.

CarePlus New Jersey has a vested interest in ensuring that its electronic equipment (i.e. computers, telephones, cell phones, blackberries and laptops), as well as its business communication tools (i.e. voicemail, email, fax and Internet) are used during working hours for business purposes, and that employees are not engaging in illegal and/or inappropriate activities in the workplace.

The Agency's Electronic Policy applies to all employees, clinical and non-clinical, and has been implemented for the protection of CarePlus, its clients and staff. Vendors of CarePlus New Jersey required to use our electronic equipment must also comply with the Agency's Electronic Policy and Procedures. This policy is consistent with and is incorporated into Chapter 10 of the CarePlus New Jersey Information Management Policies and Procedures.

Voice mail, email, and Internet usage assigned to an employee's computer, telephone extensions, cell phone and blackberry are solely for the purpose of conducting CarePlus New Jersey business. Some job responsibilities at the Agency require access to the Internet and the use of software in addition to the Microsoft Office suite of products. Only people appropriately authorized, for Agency purposes, may use the Internet or access additional software.

SOFTWARE ACCESS PROCEDURE

Software needed, in addition to the Microsoft Office suite of products, must be authorized by your supervisor and downloaded by the IT department. If you need access to software in order to carry out your work responsibilities and the software is not currently on the Agency network, talk with your supervisor and consult with the IT department. Employees are not to upload software their computers without permission and approval from his/her supervisor and the IT department designee.

Employees must adhere to copy right laws. Keep in mind, the Agency does not actually purchase software; it only purchases the license to use the software.

INTERNET USAGE

Internet use, on CarePlus New Jersey time, is authorized to conduct Agency business only. Internet use brings the possibility of breaches to the security of confidential Agency information. Internet use also creates the possibility of contamination to our system via viruses or spyware. Spyware allows unauthorized people, outside the Agency, potential access to CarePlus New Jersey passwords and other confidential information.

Removing such programs from the Agency's network requires IT staff to invest time and attention that is better devoted to the overall maintenance, improving and monitoring of the Agency's system. For this reason, and to assure the use of work time appropriately for work, we ask staff members to limit Internet use.

Additionally, under no circumstances may an Agency's computer or other electronic equipment be used to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-business-related Internet sites; to send harassing or threatening communication to others; for soliciting funds, political messages, gambling, commercial or illegal activities; for personal marketing purposes. Doing so can subject you to disciplinary action up to and including termination of employment.

EMAIL USAGE AT CAREPLUS NEW JERSEY

Email users have no expectation of privacy. All messages within or received into the CarePlus New Jersey email system are considered to be the property of CarePlus. Therefore, emails are to be used for Agency business only. CarePlus New Jersey confidential information must not be shared outside of the Agency, without authorization, at any time. You are also not to conduct personal business using the Agency computer or email. Please keep this in mind, also, as you consider forwarding non-business emails to associates, family or friends. Non-business related emails waste company time and attention.

Viewing pornography, or sending pornographic jokes or stories via email is prohibited and is considered sexual harassment and will be addressed according to our sexual harassment policy.

Unknown attachments or unrecognizable emails should not be opened.

Any unrecognizable or suspicious email should be reported to the Security designee or IT immediately.

EMAIL OF CLIENT INFORMATION

<u>For external purposes</u>

The Agency recognizes that grant funders (i.e. State/Federal/County) may require you to email specific client information to ensure program compliance. We ask that whenever possible limit email communication with the State and/or funding entity to de-identified client information and use the assigned Agency client number as a reference (assigned by Profiler, SOS, or other electronic sources). You are to avoid sending client personal, medical and/or identifying information via email unless authorized to do so by your supervisor and/or as a Federal/State/County grant requirement. If it becomes necessary to send client information, it is strongly suggested that you attach delivery and read receipts to the email.

<u>For internal</u>

For internal purposes whenever possible use the assigned Agency client number when referring to or communicating client information with co-workers.

EMAILS THAT DISCRIMINATE

Any emails that discriminate against employees by virtue of any protected classification including race, gender, nationality, religion, and so forth, will be dealt with according to the Agency harassment policies and procedures.

These emails are prohibited at CarePlus New Jersey. Sending or forwarding non-business emails may result in disciplinary action that may lead to employment termination.

COMPANY OWNS EMPLOYEE EMAIL

Email can be forwarded, intercepted, printed and stored by others. Keep in mind that CarePlus owns any and all communication sent or received via email using its equipment and/or that is stored on company equipment. Management and other authorized staff have the right to access any material in your email or on your work computer, laptop, cell phone, blackberry or any agency issued devise at any time. Please do not consider your electronic communication, storage or access to be private if it is created or stored at work.

There should be no expectation of privacy if you access your personal, password-protected, web-based email accounts or any personal email accounts, using CarePlus New Jersey equipment. This means that if you text, blog, instant message, tweet or access social networking sites such as Facebook, Twitter MySpace and the like, using CarePlus New Jersey equipment, there is not expectation privacy for that communication. Therefore, it is best not use CarePlus New Jersey equipment for personal use.

The Agency must stress the importance of using Agency equipment for business purposes. Remember the confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality.

AGENCY AUDITS

For purposes of maintaining our data systems, CarePlus reserves the right to audit and/or monitor all internal and external uses of our system, this includes auditing of Internet activities including but not limited to the right to review any employee's electronic files. This also includes auditing and monitoring the usage of Agency issued cell phones and blackberries as well. The data system audit can include the time a user is on the Internet and the web address of the visited site(s). The utilization of emails through Microsoft Outlook is also monitored.

CarePlus is constantly working on, upgrading and reviewing the data system, removing and installing information on our network for the purposes of efficiency needed to conduct business. Misuse of the Internet and Microsoft Outlook can hinder the installation and running of these applications. Therefore, it is important for all employees to understand that using the system for your own personal use has a direct effect on the overall Agency computer system. Although you may delete non-related work items, they are still stored in the Agency's system and be subject to our auditing process.

It has not been the practice of the Agency to watch employee use of the system on a daily basis; however, we reserve the right to periodically monitor your Agency issued computer, cell phone and blackberry use.

If during an IT audit or routine review of your computer or other Agency issued electronic devices, you are found to be in violation of the Electronic Policy, your immediate supervisor will be notified and further disciplinary action may be taken as outlined herein up to and including termination from employment.

GENERAL

All employees at CarePlus should respect the "confidentiality" of others electronic communications. You should not attempt to hide your identity. Nor can any employee utilize another employee's log name or password. To share your assigned log name or password is a violation of Agency policy and may subject you to disciplinary action up to and including termination.

Any CarePlus New Jersey employee found to be abusing these privileges will be subject to corrective actions that may include formal disciplinary action up to and including termination.

Any CarePlus New Jersey employee who discovers a violation of this policy must notify his/her immediate supervisor, who will in turn notify the appropriate Management and IT personnel. You may also report any concerns to the designated CarePlus New Jersey Privacy/Security Officer and/or the Corporate Compliance Officer.

PASSWORD POLICY

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or use of CarePlus New Jersey resources. All users, including contractors and vendors who are given access to the Agency's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- All CarePlus systems require a valid user ID and Password.
- Employees must agree to abide by security policies before being issued a logon ID.
- Passwords are not stored in usable form.
- Logon ID's are never shared.
- User-chosen passwords should have 5-10 characters and contain alphabetic and non alphabetic characters within the password. It is best to imbed the non alphabetic characters e.g. best998name. Do not choose a name that is easily guessed. Avoid names of sports teams, personal names and dates of birth.
- All passwords must be changed immediately if disclosed or suspected of being disclosed. Disclosure must be reported to the Agency Security designee or IT department immediately.

MOBILE DEVICE AND LAPTOP POLICY

- Devices must be password protected (laptops, phones and tablets)
- Some devices allow encryption please do if you can. If you need assistance please contact IT.
- Firewall and antivirus must be installed and auto protection is enabled.
- Do not share your agency property devices with your friends, family and children.
- Do not allow your device to remember your credentials when logged in to our terminal server, email and intranet.
- Do not leave client related information on your device, always save your work to our network.
- If internet access was not available at the time, make sure to move you documents to the network when internet access is available.
- When deleting agency related documents make sure it is also deleted from your recycling Bin.
- Try to protect your documents with a password (all Microsoft office products allow you to password protect documents).
- Logout or Lock your computer when you are away from your device.
- External storage media must not have client information or important agency information unless it is encrypted or password protected.

- Managers must not leave employee personal information on mobile devices or storage media unless it is encrypted and password protected.
- Do not share passwords with others.
- Do not save agency related documents to the clouds especially when it a free service, security normally is low or does not exist.
- Do not leave your device in your car without the prober security.
- Remember all agency issued devices must be used for business not personal usage.

WORKSTATION POLICY

Users will:

1. Report potential threats to the computer.
2. Document and report any suspicious activity, such as unknown programs appearing on the workstation.
3. Ensure that all computer equipment is plugged into a surge protector.
4. Refrain from eating and drinking at a work station.
5. Make sure no one is observing password entry or the information visible on the monitor.
6. Only access the Confidential Information required for job performance.
7. Monitor printers when printing Confidential Information. Retrieve anything containing confidential information IMMEDIATELY to avoid a *potential breach of confidentiality.*
8. Use the agency computer system and equipment only for CarePlus business.
9. Obtain authorization to download agency data or software.
10. Not install personal software onto CarePlus computers. This includes music sharing software and games as well as any unapproved software.
11. Not open files from an unknown source especially those with an external extension, i.e. do not open a file when you do not know who created the file and the reason it was created.
12. Logoff the system or lock the workstation when leaving the workstation. Logoff at the end of the day. At shift change, logout when ending the shift and login when starting the shift (Failure to log off at the end of a shift will be treated as equivalent to sharing your password.).
13. Not Use DVDs or CDs from outside the agency unless authorized by the IT Department.
14. Be responsible for the accuracy of any data input or transmitted.
15. Not share LOGIN ID's with ANYONE. If someone needs access, refer him or her to the Supervisor.
16. Not make any unauthorized transmissions, inquiries, modifications, or deletions of Confidential Information in CarePlus' computer system.
17. Obtain identification from anyone who wishes to use your computer, determine why they need your computer and do not allow them to use your login ID.
18. Report to their supervisor or the Associate VP Quality Assurance any violations of security policies. Violations may also be reported to the IT Department.
19. Understand that all computer access activity is subject to audit.
20. Make sure you Logout of your computer at the end of your shift and not Lock your computer. Logout will force the computer to close all open programs and documents, locking the computer does not do so.